IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Maino, et al.	Attorney Docket No.: ANDIP004/ 425452
Application No.: 10/034,367	Examiner: TESLOVICH, TAMARA
Filed: December 27, 2001	Group: 2137
Title: METHODS AND APPARATUS FOR SECURITY OVER FIBRE CHANNEL	Confirmation No: 8712

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on September 2, 2008.

Signed: /Latonia Ervin
Latonia Ervin

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Claims 1-25 were withdrawn from consideration. The Examiner rejected the claims 26-50 under 35 U.S.C. 103(a) as being unpatentable over Hawe (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

The Examiner argues that a "security control indicator" recited in the claims is anticipated because Hawe describes a cryptographic preamble. "More specifically, the offset field included in the cryptographic preamble indicates a number of data elements to skip to the start of the material to be cryptographically processed. In the method of the invention, this offset is used to skip over header information in the packet, which may vary in length and content depending on the protocol under which the packet was generated. The cryptographic preamble further includes a mode field indicating the type of cryptographic processing to be performed, and the step of performing the cryptographic processing includes conditioning the cryptographic processor to perform the type of processing requested in the mode field. The available modes include encrypting for outbound transmission, encrypting or decrypting for loopback to the node

processor, encrypting a cipher key for loopback to the node processor, and computing an integrity check value for loopback to the node processor." (column 3, lines 36-64)

Hagerman describes "A Fibre Channel storage area network utilizes frames having time-of-transmission and authentication-code fields. These fields are in addition to the normal fields of Fibre Channel frame headers, and may be implemented as a higher-level protocol encapsulated in the data portion of each frame or may be embedded in an enhanced frame header. The time-of-transmission field is derived from a real-time clock on each node. The real-time clock is incremented quickly enough that no two frames transmitted within a reasonable time of each other will have the same time-of-transmission field contents." (column 3, lines 23-33).

The Examiner relies on Hawe to describe "receiving a frame at a first network entity from the second network entity in a fibre channel network" and "identifying a security control indicator in the frame from the second network entity, wherein the security control indicator is used to determine if the frame is encrypted and authenticated." The Examiner argues that Hawe has a cryptographic preamble and an offset field included in the cryptographic preamble that operates as a "security control indicator."

The Applicants respectfully disagree. The cryptographic preamble and offset field are not transmitted in any frame as recited in the independent claims. The independent claims explicitly recite receiving a frame at a first network entity from the second network entity and identifying a security control indicator in the frame from the second network entity. Hawe does not teach or suggest any security control indicator that can be transmitted to a first network entity from a second network entity. Even if the cryptographic preamble and the included offset field are assumed to be the security control indicator, the cryptographic preamble is not received at a second network entity from a first network entity in a fibre channel fabric.

Hawe states that "The invention comprises the steps of appending a cryptographic preamble to the beginning of an information packet for which cryptographic processing is needed; passing the information packet to a cryptographic processor; detecting, in the cryptographic processor, that cryptographic processing is needed; analyzing the cryptographic preamble to determine the location in the packet of material to be cryptographically processed, and the type of cryptographic processing to be performed; performing the requested

cryptographic processing; and stripping the cryptographic preamble from the packet if the packet is to be transmitted onto the network, to preserve compatibility with existing packet formats transmitted over the network." (column 3, lines 15-23)

However, Hawe explicitly requires "stripping the cryptographic preamble from the packet if the packet is to be transmitted onto the network, to preserve compatibility with existing packet formats transmitted over the network." (column 3, lines 22-23) Hawe not only does not teach or suggest all of the elements of the independent claims, Hawe actually teaches away from the techniques and mechanisms of the present invention because Hawe suggests that any security control indicator such as a cryptographic preamble has to be stripped from the packet before transmitting the packet "to preserve compatibility with existing packet formats transmitted over the network." By contrast, the independent claims recite a "security control indicator" that is included in a frame transmitted between two network entities in a fibre channel network. Hawe further emphasizes this aspect by stating "The header does not affect packet formats transmitted on a network, because it (the cryptographic header) is stripped off the packet prior to transmission." (column 19, lines 27-30)

By contrast, the techniques and mechanisms of the present invention recognize that having a security control indicator allows processing even when a packet is transmitted under a standard protocol that does not support encryption. For example, "Figure 10 is a process flow diagram showing a network node in a fibre channel fabric receiving a frame. At 1001, the frame is received. At 1003, it is determined if the frame is secured. Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security. A frame that supports encryption and authentication is herein referred to as a secured frame. A frame that supports only authentication is herein referred to as an authentication secured frame. A frame that supports only encryption is herein referred to as an encryption secured frame."

That is, a conventional protocol such as a conventional fibre channel protocol can be used. In some examples, a fibre channel network node could simply ignore a security control indicator if the network node did not support encryption and authentication. "If the frame is not secured, processing proceeds using a conventional fibre channel protocol. If the frame is secured, an identifier such as a security parameters identifier SPI is referenced against a security

database such as a security association database at 1005. Key information and algorithm information are extracted from the entry containing the identifier or security parameters index associated with the received frame." According to various embodiments, the encryption method is obtained from the security association database.

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
Weaver Austin Villeneuve And Sampson LLP

/Audrey Kwan/
G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100

APPENDIX: IN THE CLAIMS

1. (Withdrawn) A method for authenticating network entities in a fibre channel network, the method comprising:

receiving a fibre channel authentication message from a first network entity at a second network entity in a fibre channel network, wherein the authentication message provides information for authenticating or reauthenticating the first network entity in the fibre channel network;

determining that both the first network entity and the second network entity support security;

verifying that the first network entity corresponds to an entry in an authentication table associated with the second network entity;

receiving first network entity verification information that confirms the identify of the first network entity.

2. (Withdrawn) The method of claim 1, further comprising generating a session key at the second network entity, wherein the session key is generated using public information associated with the first network entity and a random parameter.

3. (Withdrawn) The method of claim 1, further comprising:

exchanging security association parameters such as the SPI and the algorithm identifier.

4. (Withdrawn) The method of claim 1, wherein the authentication message is associated with a request for a fabric login.

5. (Withdrawn) The method of claim 1, wherein determining that both the first and second network entities support security comprises identifying a security enable parameter in the initialization message.

6. (Withdrawn) The method of claim 1 further comprising determining which authentication and key exchange protocol are supported by the two entities.

7. (Withdrawn) The method of claim 2, wherein the public information associated with the first network entity is provided to the second network entity by the first network entity.

8. (Withdrawn) The method of claim 2, wherein the session key generated at the second network entity is also generated at the first network entity using public information associated with the second network entity and a random parameter provided by the second network entity.

9. (Withdrawn) The method of claim 8, wherein the public information associated with the second network entity is provided to the first network entity by the second network entity.

10. (Withdrawn) The method of claim 8, wherein first network entity verification information is generated at the first network entity using public information associated with the first and second network entities and the session key.

11. (Withdrawn) The method of claim 10, further comprising verifying that the first network entity verification information received corresponds to verification information generated at the second network entity using public information associated with the first and second network entities and the session key.

12. (Withdrawn) The method of claim 11, further comprising transmitting second network entity verification information to the first network entity, wherein the second network entity verification information is generated at the second network entity using public information associated with the first network entity, the first network entity verification information, and the session key.

13. (Withdrawn) The method of claim 12, wherein the second network entity verification information transmitted corresponds to second network entity verification information generated at the first network entity using public information associated with the first network entity, the first network entity verification information, and the session key.

14. (Withdrawn) The method of claim 8, wherein the second network entity is a storage device in a storage area network.

15. (Withdrawn) The method of claim 8, wherein the first and second network entities are domain controllers in a storage area network.

16. (Withdrawn) The method of claim 8, wherein the first and second network entities are switches.

17. (Withdrawn) The method of claim 8, wherein the first network entity is a host.

18. (Withdrawn) The method of claim 17, wherein the second network entity is a storage device.

19. (Withdrawn) The method of claim 8, wherein the authentication message is a fibre channel authentication message.

20. (Withdrawn) The method of claim 19, wherein the authentication message is a login message.

21. (Withdrawn) The method of claim 20, wherein the authentication message is a PLOGI or FLOGI message.

22. (Withdrawn) The method of claim 8, further comprising:

storing security association information associated with the first network entity.

23. (Withdrawn) The method of claim 8, further comprising:

transporting security association information in the messages exchanged between the two network entities

24. (Withdrawn) The method of claim 22, wherein security association information comprises an identifier associated with the first network entity and the session key.

25. (Withdrawn) The method of claim 24, wherein security association information further comprises an encryption algorithm identifier and an authentication algorithm identifier.

26. (Previously Presented) A method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a frame at the first network entity from the second network entity in a fibre channel network;

identifying a security control indicator in the frame from the second network entity, wherein the security control indicator is used to determine if the frame is encrypted and authenticated;

determining that a security association identifier associated with the frame corresponds to an entry in a security database;

decrypting a first portion of the frame by using algorithm information contained in the entry in the security database.

27. (Original) The method of claim 26, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

28. (Original) The method of claim 27, wherein the first portion is decrypted using a key contained in the entry in the security database.

29. (Original) The method of claim 27, wherein the first portion is encrypted using DES, 3DES or AES.

30. (Original) The method of claim 27, further comprising:

recognizing that a second portion of the frame supports authentication;

using algorithm information contained in the entry in the security database to authenticate the second portion of the frame.

31. (Original) The method of claim 30, wherein the second portion is authenticated using MD5 or SHA1.

32. (Original) The method of claim 30, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

33. (Original) The method of claim 32, wherein the login sequence is a PLOGI or FLOGI sequence.

34. (Original) The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence.

35. (Original) The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a SW_ILS sequence.

36. (Previously Presented) A method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

identifying a fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

determining if the fibre channel frame corresponds to the selectors of an entry in a security database;

encrypting a first portion of the fibre channel frame using key and algorithm information associated with the entry in the security database;

providing a security control indicator in the fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated;

transmitting the fibre channel frame to the second network entity.

37. (Original) The method of claim 36, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

38. (Original) The method of claim 36, wherein the payload is encapsulated using the Authentication Header protocol or the Encapsulating Security Payload protocol.

39. (Original) The method of claim 38, further comprising adding security information to the header of the fibre channel frame.

40. (Original) The method of claim 37, wherein a first portion of the fibre channel frame is encrypted using DES, 3DES, or AES.

41. (Original) The method of claim 37, wherein parameters in the header are normalized prior to encrypting the first portion of the fibre channel frame.

42. (Original) The method of claim 41, wherein the payload is padded prior to encrypting the first portion of the fibre channel frame.

43. (Original) The method of claim 37, further comprising:

computing authentication data using key and algorithm information as well as a second portion of the fibre channel frame.

44. (Original) The method of claim 43, wherein authentication data is computed using MD5 or SHA1.

45. (Original) The method of claim 43, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

46. (Original) The method of claim 45, wherein the login sequence is a PLOGI or FLOGI sequence.

47. (Original) The method of claim 45, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence or an SW_ILS message.

48. (Previously Presented) An apparatus for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying a fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

means for determining if the fibre channel frame corresponds to the selectors of an entry in a security database;

means for encrypting a first portion of the fibre channel frame using key and algorithm information associated with the entry in the security database;

means for providing a security control indicator in the fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated;

means for transmitting the fibre channel frame to the second network entity.

49. (Original) The apparatus of claim 48, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

50. (Previously Presented) An apparatus for receiving encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying that the frame has been encrypted and authenticated;

means to lookup the security parameters in a security database that allow the de-encapsulation of the frame;

means to decrypt the eventually encrypted frame;

means to verify that the message has been sent by the sender, and that has not been tampered with during its transmission.